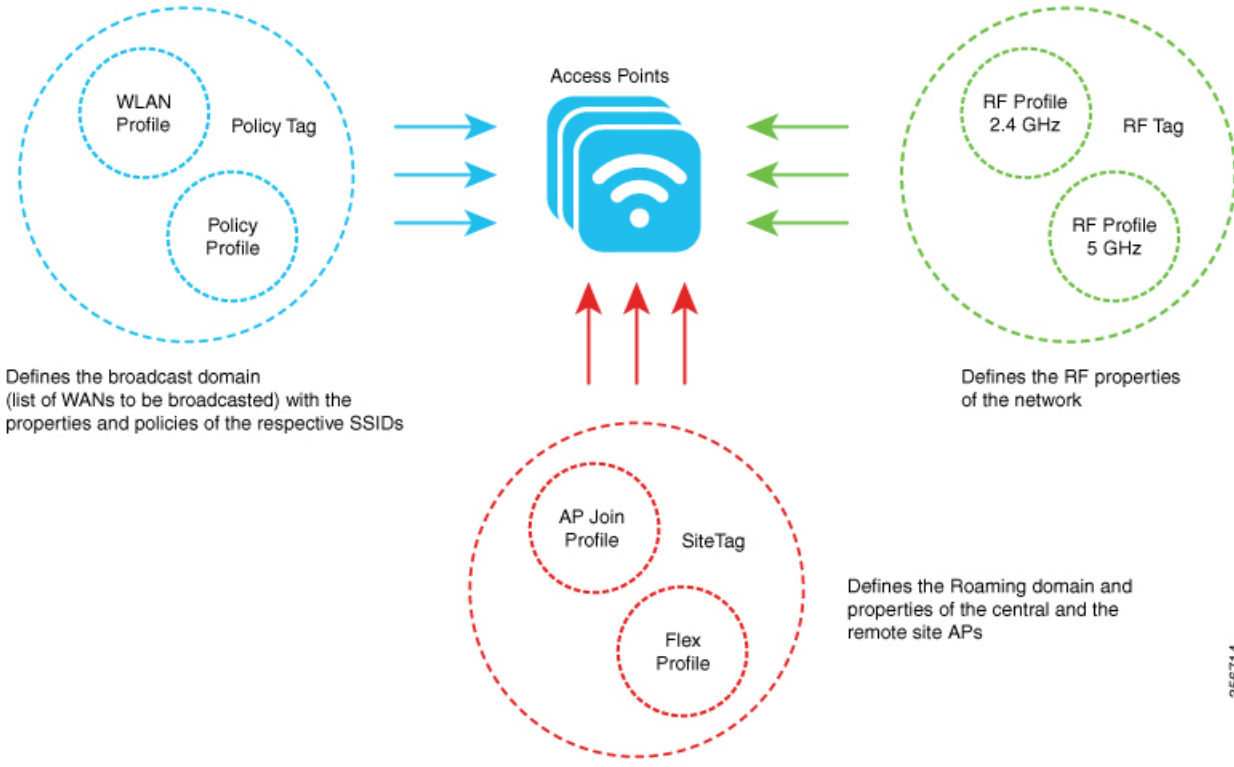
Elements of the Configuration Model

Elements of the Configuration Model

This section describes profiles and tags that constitute the configuration model.

Figure 1: Elements of the Configuration Model



Profiles

Profiles define the properties of the AP or the associated clients. Profiles are reusable entities that can be used across tags. By default, WLAN profile, Policy profile, AP Join profile, Flex profile, and 2.4/5GHz RF profiles are available on the wireless controller during boot up.

Other kinds of profiles are also available, depending on the characteristic of the network they define. These profiles are part of a larger construct called a Tag.

There are five types of profiles:

- WLAN Profile: Defines the properties of a Wireless LAN (WLAN) such as the profile name, status, WLAN ID, layer 2 and layer 3 security parameters, Authentication, Authorization, and Accounting (AAA) server associated with the service set identifiers (SSIDs), and other parameters that are specific to a particular WLAN.

  An SSID identifies the specific wireless network for the controller to access. WLAN profiles are configured with same or different SSID. Creating WLANs with the same SSID allows the assignment of different layer 2 security policies within the same wireless LAN.

  To distinguish WLANs having the same SSID, create a unique profile name for each WLAN. WLANs with the same SSID must have unique layer 2 security policies so that clients can select a WLAN based on the information advertised in the beacon and probe responses. The switching and network policies are not part of the WLAN profile.

- Policy Profile: Defines the network policies and the switching policies for a client with the exception of quality of service (QoS), which constitute the AP policies. Policy profile is a reusable entity across tags. Anything that is a policy for the client that is applied on the AP or controller is moved to the policy profile. For example, VLAN, access control list (ACL), QoS, session timeout, idle timeout, Application Visibility and Control (AVC) profile, Bonjour profile, local profiling, device classification and so on. Switching policies define central switching or local switching attributes of a WLAN.

  The WLAN profile and Policy profile are both part a Policy Tag and define the characteristics and policy definitions of a set of WLANs.

- AP Join Profile: Consists of the following parameters, Control and Provisioning of Wireless Access Points (CAPWAP) IPv4 or IPv6 , UDP Lite, high availability, retransmit configuration parameters, global AP failover, hyperlocation configuration parameters, Telnet or SSH, 11u parameters, and so on. The default AP join profile values have the global AP parameters and the AP group parameters. Some AP join profile changes require the CAPWAP connection to be reset, because these parameters pertain to the characteristics of the AP.

- Flex Profile: Groups all settings to be assigned to a Flex AP, native VLAN, ACL mapping, and so on. It contains policy attributes and remote site-specific parameters. For example, the Extensible Authentication Protocol (EAP) profiles that can be used when the AP acts as an authentication server.

  The AP Join profile and Flex profile are both part of a Site Tag and define the characteristics of a local or remote site.

- Radio Frequency (RF) Profile: Contains the common radio configuration for APs. RF profiles are applied to all the APs that belong to an AP group, where all the APs in that group have the same profile settings. By default, there exists two default RF profiles, one for 802.11a and one for 802.11b.

Tags

A tag is defined by the policies associated with it. The properties of the tag is in turn inherited by an associated client or AP. There are various types of tags, each associated with different profiles. No two types of tags include profiles having common properties. Each tag has a default that is created when the system boots up.

- Policy Tag: Defines network and switching policies for the client. QoS is an exception, which constitutes AP policies as well. Policy tag maps the WLAN profile to the policy profile.

  This tag contains the map of the WLAN policy profile. There are 16 entries per policy tag. Changes to the map entries are based on the status of the WLAN profile and policy profile. For example, if a map is added to the policy tag, and both the WLAN profile and the policy profile are enabled, the definitions are pushed to APs using the policy tag. However, if one of them is in the disabled state, the definition is not pushed to the AP. Similarly, if a WLAN profile is already being broadcast by an AP, it can be deleted through the CLI in the policy tag.

- Site Tag: Assigns the AP Join profile settings to the AP. The site tag defines the properties of a site, both central and remote (FlexConnect) site. The attributes of a site that are common across central and remote site are part of the AP Join profile. The attributes that are specific to flex or remote site are part of the Flex profile. The default Site Tag constitutes of the default AP Join profile. There is no default Flex profile.

  Apart from the Flex profile, the site tag also comprises of attributes that are specific to the physical site (and hence cannot be a part of the profile that is a reusable entity).

  If a Flex profile name or an AP profile name is changed in the site tag, the AP is forced to rejoin the controller by disconnecting the Datagram Transport Layer Security (DTLS) session. When a site tag is created, the AP and Flex profiles are set to the default values, default-ap-profile and default-flex-profile.

- RF Tag: Contains the 2.4 GHz and 5 GHz RF profiles. The default RF tag contains the global configuration. Both these profiles contain the same default values for global RF profiles for the respective radios.

An access point is always assigned three tags, one for each type. If a tag is not explicitly defined, the AP will get the default policy, site, or RF tag.

Roaming Between Policy Tags

Policy tags are used to verify the SSID that is being broadcast by an AP, and the type of policy, so that policy tags define the broadcast domain for a group of APs.

Roaming across two different policy tags (the same SSID, but different policy profile name) or intra-controller roaming will force a client to go through the full authentication and DHCP process to renew its IP address. The process is to prevent clients from jumping from one policy to another without a full reauthentication.

Note If a policy profile associated to an SSID is the same (same name and content) in different policy tags, then roaming for that SSID is seamless. The slow roam happens if there is a change in the policy profile associated to the SSID.

Assigning Tags to Access Points

You can assign tags from the following sources. The sources are listed in the order of priority.

- Static: You select an AP and assign tags. This configuration is saved on the controller based on the AP's Ethernet MAC address. When an AP joins the specific controller, it is always assigned the specified tags.
- Location: This is a configuration construct internal to the Cisco Catalyst 9800 Series Wireless Controller (It is not the AP location that you can configure on each AP.), and is used primarily in the basic setup flow. A location allows you to create a group of three tags (policy, site, and RF) and assign APs to it.
- Filter: You can use a regular expression to assign tags to APs as they join the controller. You can set a filter based only on the AP name, so that this method cannot be used for out-of-the-box APs.
- AP: The AP itself carries the tag information learned through Plug-and-Play (PnP) or pushed from the controller.
- Default: This is the default tag source.

The first two methods of assigning tags (static and location) are static mapping configurations, and hence have the highest priorities. Filter allow you to define a dynamic mapping of APs-to-tags based on regular expressions. When the source is an AP, it means that this information is saved on the AP itself and will be presented to the controller when the AP joins it. If there is no tag mapping configuration on the Cisco Catalyst 9800 Series Wireless Controller, and if APs do not carry any tag information, these APs are assigned default tags.

Access Points are tagged based on the broadcast domain, the site it belongs to, and the desired RF characteristics. Once tagged, the AP gets a list of WLANs to be broadcast along with the properties of the respective SSIDs, properties of the APs on the local or remote site, and the RF properties of the network. By default, an AP is tagged with the default policy, site, and RF tag unless changed. When a tag associated with an AP is changed, the AP resets its CAPWAP connection.

APs are identified by the Ethernet MAC address, and the association to AP and tag is stored in the controller configuration.

Each AP is assigned three unique tags: a policy, site, and RF tag. By default, when an AP joins the controller, it gets default tags; the default policy tag, default site tag, and default RF tag. You can change to the default tags or create custom tags. Use the WebUI to view the tags configured on each AP.

Preserving Tags When Moving APs Between Controllers

The following conditions must be met when moving APs between controllers:

- If the AP does not have any tag information and there is no mapping configured for that AP on the controller to be joined, the AP is assigned default tags when moved to the controller.
- The AP retains the tag information when moving between the controllers, if both the controllers have the same mapping of AP to the tags. This can be done through static configuration, by assigning the AP to a location, or through filters.
- The AP retains its tag when moved between the two controllers if the tags are saved to the AP and the tags are defined on both controllers.
- If the AP has a saved tag assigned and joins a controller where these tags are not present, the AP is assigned default tags (assuming that no other mapping is configured on the controller that the AP is joining).
- If the AP retains its tag name assignment, but the settings within the tag are different on the two controllers, the AP is configured based on the settings present on the currently joined controller.

Note The above information also applies to N+1 redundancy.

AP Filter

AP filters are similar to the ACLs used in the controller, and are applied at the global level. You can add AP names as filters, and other attributes can be added as required. You can also add the filter criteria as part of the discovery requests.

The AP Filter feature organizes tag sources with the right priority, based on the configuration.

You cannot disable the AP filter feature. However, the relative priority of a tag source can be configured using **ap filter-priority** *priority filter-name* command.

Note You can configure tag names at the Plug-n-Play (PnP) server (similar to the Flex group and AP group), and the AP stores and send the tag name as part of the discovery and join requests.

Modifying Access Point Tags

Modifying an AP tag results in the DTLS connection being reset, forcing the AP to rejoin the controller. If only one tag is specified in the configuration, default tags are used for other types. For example, if only policy tag is specified, the default site tag, and default RF tag are used for the site and RF tags.

RF Tag Profiles

RF Profiles allows you to group set of APs that share a common coverage zone together and selectively change how RRM operates the APs within that coverage zone. For example, a university might deploy a high density of APs in an area where a high number of users congregate or meet. This situation requires that you manipulate both data rates and power to address the cell density while managing the co-channel interference. In adjacent areas, normal coverage is provided and such manipulation would result in a loss of coverage.

Using RF profiles and RF tags allows you to optimize the RF settings for set of APs that operate in different environments or coverage zones. RF profiles are created for the IEEE 802.11 radios and are applied to all APs that are mapped to an RF tag, where all APs with that RF tag have the same profile settings.